OSG Summer Workshop
Lubbock, 2011

Security Brief

Anand Padmanabhan
for the OSG Security team

What is security?

- Security is much more than just technology
  - It is as much a social problem
- We have a secure system only if the participants act responsibly
- Malicious participants are obviously removed from the system
  - But a careless one can make almost as much damage!
- Know your responsibilities
  - https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/SecuritySiteResponsibilities

Site Responsibilities

- Keep security contact information in OIM updated
- Read Security Notifications from OSG
- Know your institutional cyber security officer
- Apply security updates of VDT/OSG software
- Maintain up-to-date Trusted CA information
- Maintain up-to-date VO and user access information
- Reporting and Responding to Security Incidents
- Respond to requests from the OSG Security Officer
- Learn how to communicate securely
- Be familiar with the OSG Security web site
- Review log files regularly

How to get hold of us

- If you suspect a compromise, immediately notify the OSG security team
  https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/IncidentDiscoveryReporting
  - Even if it turns out that it was a false alarm, better safe than sorry
- Involving your local Campus/Institutional security team is a good idea

Security communication

- Security contacts will receive security notifications through e-mail
  - Please read and act upon them
  - Make sure they have a legitimate signature
    https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/OSGSecurityNotifications
- Know and possibly be in contact with your Campus/Institution cyber security team
  - They can provide invaluable help both in preventing and fixing security incidents

Leasons for a recent incident

- Recently we observed a new sophisticated attack on HPC site
  - Discovered large portion of cluster was running malicious processes
  - Someone used a scientific cluster for profit
  - Is this a new trend? We don't know but we want you to be vigilant
- How was the attack caught
  - ps was rootkitted and the attackers were cleaning the logs, so admin thought everthing was OK
  - There were constant user complaints that they were not getting enough cpu time on system
  - Following up, the site admin noticed some differences in utilization reports

What can you do?

- Users:
  - Initial compromise was though user account
    - Protect your account!
  - Discovered by unaccounted for process utilization
    - Keep an eye on your usage reports
- Admins:
  - Watch authentication logs
  - Log to central syslog server if possible
    - logs were removed by miscreants
  - Account for processes on systems
  - Do file integrity checking
  - Monit can do lightweight process, file, and disk accounting

Best Practices

- Keep all the software up-to-date
  (mostly patching, but also upgrades as needed)
  - Operating system, System services, OSG/VDT software
- Keep security data up-to-date
  - Trusted CAs list, Associated CRLs, list of Supported VOs
- Run only minimal set of services
- Keep eye on monitoring and usage data
- Do not allow interactive user access to gatekeeper and/or worker node
  - If unavoidable restrict access to small group of users/subnet

Rest of this Workshop

- Tomorrow we have a presentation in the user forum titled: Security - infrastructure, certificates and responsibilities
- I will be here today and tomorrow
  - Talk to me if you have any questions or concerns related to OSG security

Credits

- Mine Altuay
- James Barlow
- Igor Sfiligoi

Thank YOU!!